

Cybersecurity Education: Why Universities are Missing the Mark



Latest estimates show that by 2021, the vacancy rate in Cyber Security worldwide will reach 3.5 million. There are many causes contributing to the cybersecurity skills gap – which continues to grow – but top of the list is Cyber Security education.

Email Cyber Security is not a priority for the majority of universities



A recent study revealed how universities are missing the mark when it comes to Cyber Security education. The 121 top-ranked schools surveyed were awarded a combined grade 'F' (they've got the statistics to prove it!) To illustrate, out of the top 50 computer science programs in the US, only three require students to complete a Cyber Security course for graduation.

Here's what's contributing to the issue

Learners cannot be taught cybersecurity in a passive classroom setting because the cyber world evolves too fast

Not only are there not enough qualified educators to keep up with demand, but new cyber threats emerge every day and curriculums cannot adapt fast enough.

Cybersecurity is best learned in real time with hands-on practice

One of the biggest drawbacks is that classroom learning is non-interactive. While passive classroom learning has the advantages of lecture notes, concrete conceptual education, and organised learning, it does not challenge the learner as much as active learning. Furthermore, quizzes and exams that measure success in university are not meant to teach, they are meant to test and can't be equated to hands-on practice.

Active learning, on the other hand, increases critical thinking skills, initiative, and better fits the needs of fluctuating learning styles. Active learning, most importantly, puts knowledge to practice. Labs and simulations are engaging and more effective for internalising and building confidence in applied knowledge. These are all vital hard and soft skills for being successful in a cybersecurity career.

Universities are exclusive

The assessments and grading required to get into and succeed in university is also generally irrelevant to cybersecurity. There are many potential individuals who are left out of the university system whether it be from entry requirements or cost. Adding insult to injury, women are still highly underrepresented in cybersecurity, and that starts with university recruitment, outreach, and retention.

Lastly, cybersecurity requires continuous learning and on-the-job training. While university training remains the most popular route into the cybersecurity industry, it certainly won't help to solve the cyber skills gap nor help fend off the growing threats cybercriminals pose. Solving the cyber skills gap is an industry-wide problem that needs a wholesome solution. IACD's cloud-based platform is helping to solve the cyber skills gap through gamified, role-based training that keeps learners up-to-date with new skills, technologies, and threats. Contact us to find out how simple it is to implement our learning paths in your institution or organisation.

The Institute of Advanced Cyber Defence aims to advance both the quantity and quality of knowledge and skills in the domain of cyber intelligence and security. With the WEF consistently ranking 'cyber' in the top of their annual Global Risk Reports, and the (ISC)² estimating the shortage of 'cyber' professionals at 3 million globally, there is a clear mismatch between organisational needs and available talent. It is the IACD's mission to bridge this gap and address the dearth of cyber defence competencies.

The Institute's expertise is based on first-hand experience protecting organisations from cyber threats and attacks, as well as on the expertise of a network of companies from tier-1 countries that are global leaders in advanced cyber defence services and solutions. Their offerings are military-grade and find their origins in law enforcement and national security, with their team members often having served in leadership positions in the world's elite national cyber defence units.

As such, our pedigree is unmatched and with our partners we seek to further develop and transfer this know-how for the benefit of individuals and organisations alike via a number of avenues.

For more information, please contact training@iacd.io

